

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-319936

(43)Date of publication of application : 31.10.2002

(51)Int.Cl.

H04L 9/36
G09C 1/00
H04L 12/22
H04L 12/56

(21)Application number : 2001-122610

(71)Applicant : NTT DOCOMO INC

(22)Date of filing : 20.04.2001

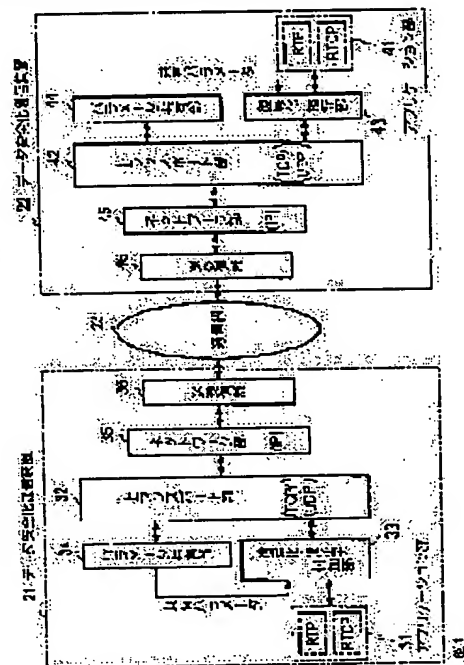
(72)Inventor : SUZUKI TAKASHI
YOSHIMURA TAKESHI

(54) APPARATUS AND METHOD FOR COMMUNICATION FOR MAKING DATA SAFE

(57)Abstract:

PROBLEM TO BE SOLVED: To enable header compression in the case of mobile communication by selectively encrypting data and generally applying them to an application on a UDP.

SOLUTION: Each of parameters indicating encryption except for a header together with an encryption algorithm or the like is shared with opposite apparatus by communication by a parameter sharing part 34 and while using the shared parameter, an identifier for data identification to an entire RTP packet from an application part 31 is calculated by an encryption/identifier adding part 33. Then, the identifier is added to the RTP packet and the data of a part except the header are encrypted and outputted to a transport part 32. In this transport part, a UDP header is added to a non-enciphered RTP header and a UDP packet is generated and sent to a network part 35.



LEGAL STATUS

[Date of request for examination]

29.09.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

BEST AVAILABLE COPY

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-319936
(P2002-319936A)

(43) 公開日 平成14年10月31日 (2002. 10. 31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/36		G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 12/22	5 K 0 3 0
H 0 4 L 12/22		12/56	3 0 0 A
12/56	3 0 0	9/00	6 8 5

審査請求 未請求 請求項の数15 O L (全 10 頁)

(21) 出願番号 特願2001-122610 (P2001-122610)

(22) 出願日 平成13年4月20日 (2001. 4. 20)

(71) 出願人 392026693

株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番1号

(72) 発明者 鈴木 敬

東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内

(72) 発明者 吉村 健

東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内

(74) 代理人 100066153

弁理士 草野 卓 (外1名)

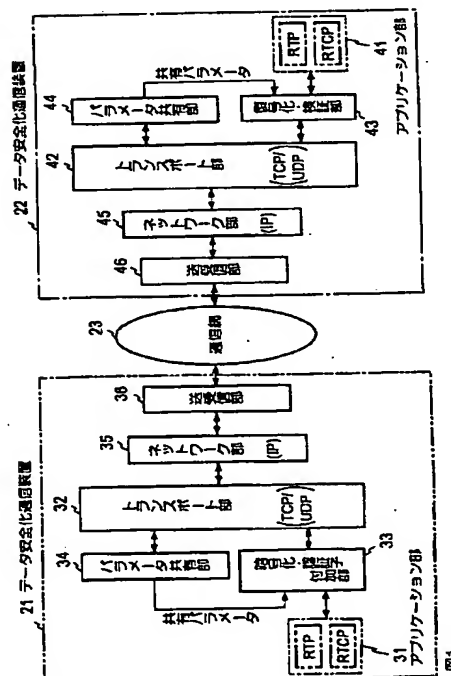
Fターム(参考) 5J104 AA08 AA33 LA01 PA07
5K030 GA15 HA08 JA05 LD19

(54) 【発明の名称】 データ安全化通信装置及びその方法

(57) 【要約】

【課題】 選択的に暗号化し、かつUDP上のアプリケーションに汎用的に適用でき、移動通信におけるヘッダ圧縮を可能とする。

【解決手段】 パラメータ共有部34により暗号化アルゴリズムなどと共にヘッダを除く暗号化であることを示す各パラメータを相手装置と通信により共有し、その共有したパラメータを用いて、暗号化・認証子付加部33でアプリケーション部31からのRTP packets全体に対するデータ認証のための認証子を計算し、その認証子をRTP packetsに付加し、そのヘッダを除いた部分を暗号化してトランスポート部32へ出力し、ここでUDPヘッダを前記非暗号化RTPヘッダに付けてUDP packetsを作ってネットワーク部35へ送出する。



1

【特許請求の範囲】

【請求項 1】 通信路を介して入力データの安全化対象を示すパラメータを相手のデータ安全通信装置と共有するパラメータ共有手段と、

前記共有されたパラメータに従って前記入力データの一部を選択的に安全化して出力する安全化手段とを備えたことを特徴とするデータ安全化通信装置。

【請求項 2】 請求項 1 に記載の装置において、入力データの種別（アプリケーション）に応じて上記安全化対象を決定する手段を備えたことを特徴とするデータ安全化通信装置。

【請求項 3】 請求項 1 または 2 に記載の装置において、この装置が接続された網の伝送特性に応じて上記安全化対象を決定する手段を備えたことを特徴とするデータ安全化通信装置。

【請求項 4】 請求項 1 乃至 3 の何れかに記載の装置において、前記安全化対象は暗号化対象であり、前記相手のデータ安全化通信装置は暗号復号化装置であり、前記安全化手段は暗号化手段であることを特徴とするデータ安全化通信装置。

【請求項 5】 請求項 4 に記載の装置において、前記入力データは RTP パケットであり、前記暗号化対象は RTP ヘッダを除くデータであることを特徴とするデータ安全化通信装置。

【請求項 6】 請求項 4 に記載の装置において、前記暗号化対象を決定する基準は、前記網の通信路の伝送速度であることを特徴とするデータ安全化通信装置。

【請求項 7】 請求項 1 乃至 3 の何れかに記載の装置において、前記安全化対象は前記入力データの認証処理範囲であり、前記相手のデータ安全化通信装置はデータ検証装置であり、前記安全化手段は前記入力データのうち前記認証処理範囲から認証子を計算する手段であり、入力データに前記認証子を付加して出力する手段とを含むことを特徴とするデータ安全化通信装置。

【請求項 8】 通信路を介して受信データの暗号復号化対象を示すパラメータを相手のデータ安全化装置と共有する手段と、受信データのうち、前記共有されたパラメータに従って一部を選択的に復号化する暗号復号化手段と、を備えることを特徴とするデータ安全化通信装置。

【請求項 9】 通信路を介して受信データの認証範囲を示すパラメータを、相手の認証子付加装置と共有する手段と、受信データのうち前記パラメータに従って前記認証範囲のデータと前記受信データに含まれる認証子から前記認証範囲に含まれるデータの正当性を検証する検証手段

2

と、を具備することを特徴とするデータ安全化通信装置。

【請求項 10】 通信路を介して入力データの暗号化対象を示すパラメータを相手暗号復号化装置と共有する過程と、

前記共有したパラメータに従って前記入力データの一部を選択的に暗号化して出力する過程とを有するデータ安全化通信方法。

【請求項 11】 請求項 10 に記載の方法であって、前記入力データは RTP パケットであり、前記選択的暗号化を、前記 RTP パケットの RTP ヘッダを除くデータに対して行うことを特徴とするデータ安全化通信方法。

【請求項 12】 通信路を介して入力データの認証処理範囲を示すパラメータをデータ検証装置と共有する過程と、

前記入力データのうち前記パラメータで指定された部分から認証子を計算する過程と、

前記入力データに前記認証子を付加して出力する過程とを有するデータ安全化通信方法。

【請求項 13】 通信路を介して受信データの暗号復号化対象を示すパラメータを相手の暗号化装置と共有する過程と、

受信データのうち、前記共有されたパラメータに従って一部を選択的に暗号復号化する過程とを有することを特徴とするデータ安全化通信方法。

【請求項 14】 請求項 13 に記載の方法において、前記受信データは RTP パケットであり、前記選択的暗号復号化を、前記 RTP パケットの RTP ヘッダを除くデータに対して行うことを特徴とするデータ安全化通信方法。

【請求項 15】 通信路を介して受信データの認証範囲を示すパラメータを、相手の認証子付加装置と共有する過程と、

受信データのうち前記パラメータに従って前記認証範囲のデータと前記受信データに含まれる認証子から前記認証範囲に含まれるデータの正当性を検証する過程とを有することを特徴とするデータ安全化通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、伝送データの傍受、改変などに対するデータの安全化、つまり暗号化、データ認証を行う通信装置及びその方法に関する。

【0002】

【従来の技術】 インターネットに代表される IP（インターネットプロトコル）ネットワークには本来セキュリティ機能が備わっていない。何ら対策を施さない場合、途中経路における IP パケットの取得や改変などにより、通信の当事者に知られずに通信内容の傍受、改変が可能である。このため、IP ネットワーク上で商取引な

どの重要情報を送受信する場合には、いかにセキュリティ（安全性）を保つかが重要な課題となる。

【0003】例えば、音楽や映像をインターネット経由で配信するコンテンツ配信サービスでは、配信される音楽・映像データが価値をもった重要情報となり、途中経路における傍受、改変を防ぐ必要がある。また、IPネットワークを介して電話サービスを提供するVoIPシステムにおいては、通話内容の不法な傍受を防ぐ必要がある。VoIPシステムやストリーム型コンテンツ配信システムにおいては、リアルタイム性（実時間性）が要求されるデータを伝送するために、RTP/UDPが一般的に利用されている。RTP（Realtime Transport Protocol）はアプリケーション層で用いられるプロトコルであり、実時間処理に適する。UDP（User Datagram Protocol）はアプリケーション層とネットワーク層とのインターフェースであるトランスポート層に用いられるコネクションレスプロトコルである。RTP/UDPでは、TCP（Transmission Control Protocol、トランスポート層で用いられるコネクション型プロトコル）のようにパケットの確実な送達よりも、即時性のあるパケットの送達を目的としているため、途中経路でパケットの送達（紛失）が生じる可能性がある。このため、RTP/UDPに適用するセキュリティ技術を検討する際には、パケットロスに対する対策が必要となる。

【0004】また、現在急速に普及している移動通信への適用も重要である。移動通信網でRTP/UDPパケット伝送を行う際には、無線伝送帯域の利用効率改善のために、無線リンクにおいてRTPパケット及びUDPパケットの両ヘッダは対ヘッダ圧縮が適用される。従って、セキュリティ技術、特に暗号化方式を検討する際には途中のリンクにおけるRTP/UDPパケットのヘッダ圧縮が可能である方式が望まれる。移動通信網への適用を前提としたRTPパケットのセキュア（安全）な伝送方式として、IETF（インターネット標準化推進団体）においてSecure RTP（SRTP、参照：draft-ietf-avt-srtp-00.txt）が提案されている。SRTPでは、ヘッダ圧縮を適用可能とするための選択的暗号化やパケットロスやビット誤りの影響が少ない暗号化方式などが導入されている。つまりRTPパケットに対し、図11に示すように、RTPヘッダを除き、RTPペイロードの部分だけを暗号化し、この暗号化されたRTPペイロードとRTPヘッダに対して、データ認証コード（認証子）を生成し、これを付加して、RTPヘッダと暗号化RTPペイロードのデータの正当性を検証可能にしている。このため、効率的な保護が可能であるが、その一方RTPに特化した技術となっている。つまりSecure RTPを使用する場合は図12Bに示すように、RTPに特化した暗号化アルゴリズム暗号化パラメータが用いられるため、他のUDP上のアプリケーション、トランスポートプロトコルにそのSecure

e RTPを用いることはできない。選択的暗号化パラメータ、暗号化アルゴリズムが固定であり、新規プロトコルに対応できない他の技術進歩の早いコンテンツ配信には適さない。このようにあるアプリケーションに特化したセキュリティ技術は、新規アプリケーションが開発される度に個別のセキュリティ技術を検討する必要がある、好ましくない。また、安全性技術は永久的ではないためSecure RTPは暗号化アルゴリズムなども固定であり、セキュリティ上問題がある。

10 【0005】一方、インターネットで広く利用されているセキュリティ技術としてSSL（Secure Socket Layer）（TSL）がある。つまりSSL（TSL）を使用しない状態では図13Aに示すようにアプリケーション層におけるHTTP（Hypertext transfer Protocol）、FTP（File Transfer Protocol）、Telnet（遠隔ログイン）などのアプリケーション層とTCP又はUDPのトランスポート層とが直接接続される。図13Bに示すようにSSLは、TCPやUDPなどのトランスポート層とアプリケーション層との間に位置するセキュリティプロトコルである。SSLは、TCPやUDPが提供するデータ伝送機能を利用して送受信されるデータに何らかのセキュリティ処理を施すことで、アプリケーション層に対してセキュアなデータ伝送サービスを提供する。このため、利用できるアプリケーション、暗号化アルゴリズムが限定されないという特徴を備える。SSLは、特にWebアクセスで使用されるHTTPセッションを保護するために広く用いられているが、FTPやTelnetなど他のアプリケーションにも汎用的に利用できる。また、SSLを移動通信用に修正したものと

30 して、WAP Forumで規格化されたWTSLがある。

【0006】SSLやWTSLは、図14に示すように大きく分けて2層構造になっている。この2層中の下位層で使用されるプロトコルはレコードプロトコル（Record Protocol）と呼ばれており、上位層のプロトコルのデータを暗号化する機能およびデータ認証コード（MAC）を付加する機能を提供する。SSLの2層構造中の上位層にはハンドシェイクプロトコル（Handshake Protocol）、アラートプロトコル（Alert Protocol）、チェンジサイファプロトコル（Change Cipher Protocol）、アプリケーションデータプロトコル（Application Data Protocol）の4種類が含まれる。ハンドシェイクプロトコルは暗号化・データ認証方式のネゴシエーション機能および端末・サーバの認証機能を有し、アラートプロトコルはイベントやエラーの通知機能を有し、チェンジサイファプロトコルはネゴシエーションした暗号化・認証方式を有効にする機能を有する、つまり暗号通信の開始を相手に通知するアプリケーションデータプロトコルは、上位のアプリケーションデータを透過的に送受信するものであり、HTTPやFTPなどのデータはこのブ

5

ロトコルを介してレコードプロトコル (Record Protocol 1) に受け渡される。

【0007】図5に送信側と受信側のレコードプロトコル (Record Protocol) 間で送受信されるデータ構造の例を示す。ヘッダ10には上位プロトコル種別 (ハンドシェーク、アラート、アプリケーションデータなど) を示す識別子 (Protocol type) 11、SSLのバージョン (Major Version、Minor Version) 12、データ長 (Length(high)、Length(low)) 13が、ペイロードには暗号化された上位プロトコルのデータ14が含まれて
10 いる。暗号化データ14中はデータ本体 (Content) とこのデータ本体及びヘッダの正当性検証用認証子MACが含まれている。この構造はレコードプロトコルを利用するプロトコル全てに適用されるものであり、アプリケーションプロトコルも例外ではない。従って、SSLを利用してRTPパケットを伝送する場合には、RTPパケットのヘッダ及びペイロードの全体が暗号化されて、レコードプロトコルデータのペイロード14にマッピングされる事となる。

【0008】このように、RTPパケット全体を暗号化したものに、もしくはRTPパケットにレコードプロトコルのヘッダを付加した場合、途中経路におけるRTPヘッダ圧縮の適用が不可能になる。つまりヘッダ圧縮は、連続して設けられているRTPヘッダとUDPヘッダとIPヘッダとを一括して行うため、RTPヘッダとUDPヘッダとの間にレコードプロトコルヘッダ10が挿入されていると、これらを一括してデータ圧縮することができなくなる。このため、SSL/WTLSをRTPパケットの保護に適用することは、移動通信において
20 は望ましくない。

【0009】

【発明が解決しようとする課題】また一般のデータの通信においても、特に安全にしたい部分に対してのみ、暗号化や正当性を検証できる認証を付けるなどの安全性を施して通信することができれば、便利であるが、その安全性を適応的に付けることは困難であった。この発明の目的は入力データの一部にのみ選択的に安全性を施して通信することを可能にするデータ安全化通信装置及びその方法を提供することにある。

【0010】

【課題を解決するための手段】この発明によれば、入力データの安全化対象を示すパラメータを相手のデータ安全化通信装置と通信路を介して共有し、この共有されたパラメータに従って入力データの一部を選択的に安全化して出力する。

【0011】

【発明の実施の形態】第1実施形態

図1にこの発明の第1実施形態を示すと共にその実施形態を用いたデータ伝送システムの概観を示す。例えばサーバやデータ端末などのこの発明による送信側のデータ
50

6

安全化通信装置21と、同様にサーバやデータ端末などのこの発明による受信側のデータ安全化通信装置22とが通信網23を通じて接続することができる。通信網23は1つの網として示しているが、公衆通信網とインターネット網とが組合された網など、複数網から構成されていてもよい。

【0012】データ安全化通信装置21はアプリケーション部31とトランスポート部32との間にこの実施形態では安全化手段として暗号化・認証子付加部33が設けられる。またトランスポート部32の上位層としてパラメータ共有部34が設けられる。トランスポート部32はTCPやUDP機能を有し、例えばIP機能を有するネットワーク部35と接続され、ネットワーク部35は物理層である送受信部36に接続され、送受信部36は通信網23と接続される。データ安全化通信装置22もデータ安全化通信装置21とほぼ同様に構成され、つまりアプリケーション部41、トランスポート部42、ネットワーク部45及び送受信部46を備え、この実施形態では安全化手段として復号化・検証部43が設けられ
またトランスポート部42の上位層としてパラメータ共有部44が設けられる。

【0013】通信装置21はアプリケーション部31からのアプリケーションデータの送信に先立ち、データ安全化に必要なパラメータ、つまり暗号化処理・データ認証子 (コード) 生成処理に必要なパラメータを通信相手の装置22と交渉して、これらのパラメータを相手通信装置22と共有する。このパラメータの例えば図2に示すように暗号化アルゴリズムを、Null、DES、3DES、RC4などの何れにするか、データ認証子生成アルゴリズムをMD5、SHAなどの何れにするか、鍵を生成するために用いる秘密情報、通信装置21 (例えばサーバ側装置) 及び通信装置22 (例えばクライアント側装置) における暗号化・復号化あるいは認証・検証に用いるランダム値、送信データ中の暗号化する範囲、データ認証する範囲などである。この実施形態では特にこの共有するパラメータとして暗号化範囲及びデータ認証範囲を新たに設けた点が重要であり、他のパラメータを共有することは、従来のSSL (TLS) による安全化プロトコルで用いられる共有パラメータと同様のものであり、またこれらパラメータの共有は、従来のSSLと同様に通信路を介して、通信装置21と22が相互に通信して行う。

【0014】ここで新たに用いる共有パラメータである、伝送すべきデータの安全化対象を示すパラメータ、この例では暗号化範囲及びデータ認証範囲は、入力データパケット (この例ではアプリケーション部31よりのデータパケット) のどの範囲を暗号化、認証するかを決定するための情報であり、様々な指定方法が考えられるが、例えば「パケット先頭の何バイト目から暗号化を開始する」などにより指定する。更にこの暗号化範囲、デ
50

ータ認証範囲の決定は入力データの種別、つまりこの例ではアプリケーションに応じて、あるいは通信装置 21 が接続された通信網 23 の伝送特性（伝送速度、遅延特性、伝送誤り特性、減衰特性、周波数特性、歪特性など）に決定される。

【0015】通信装置 21 のパラメータ共有部 34 では、例えば図 3 に示す手順により安全化対象を示すパラメータを共有決定する。暗号化通信要求を受信すると（S1）、入力データアプリケーションパケットが RTP パケットであるかを調べ（S2）、RTP パケットであれば、装置 21 が接続されている通信網 23 が伝送速度が低い網、例えば移動通信網であるかを調べ（S3）、移動通信網であれば、RTP パケットを選択的に暗号化すると、例えば入力データ先頭の RTP ヘッダを暗号化対象外とすることを示す暗号化・認証パラメータを相手通信装置 22 へ送信する（S4）。なおこの際に暗号化アルゴリズム、データ認証子生成アルゴリズムなど他のパラメータも送信する。

【0016】一方相手通信装置 22 のパラメータ共有部 44 では例えば図 4 に示すように通信装置 21 から暗号化・認証パラメータを受信すると（S1）、受信した通信相手の暗号化・認証パラメータが RTP パケット選択的暗号化であるかを調べ（S2）、そうであれば、パラメータ共有部 44 における暗号化・認証パラメータを RTP パケット選択的暗号化に決定し（S3）、その決定した暗号化・認証パラメータを通信装置 21 へ送信する（S4）。通信装置 21 のパラメータ共有部 34 では、図 3 に示すように通信装置 22 から RTP パケット選択的暗号化を示す暗号化・認証パラメータを受信すると（S5）、暗号化・認証パラメータを RTP パケット選択的暗号化に決定する（S6）。このようにして両パラメータ共有部 34、44 において暗号化・認証パラメータとして RTP パケット選択的暗号化が通信路を介して共有される。なお暗号化アルゴリズムなど他のパラメータも同様にして同時に決定される。この場合、例えば従来の SSL などと同様に、各パラメータについていくつかの候補を送って、相手装置 22 により決定してもらう。

【0017】図 3 において、ステップ S2 で入力データが RTP パケットでない判定され、あるいはステップ S3 で通信装置 21 が接続されている通信網 23 の伝送速度が高いと判定された場合は、この例では入力データ（パケット）全体を暗号化する、つまり非選択的暗号化を示す暗号化・認証パラメータを相手通信装置 22 へ送信する（S7）。通信装置 22 のパラメータ共有部 44 では図 4 に示すように、ステップ S2 で受信した通信相手の暗号化・認証パラメータが RTP パケット選択的暗号化でない判定されると、通信装置 22 のアプリケーション部 41 からの入力データ（アプリケーション）が RTP パケットであるかを判断し（S5）、RTP パケ

ットであれば、通信装置 22 が接続された通信網 23 が伝送速度の低い、例えば移動通信網であるかを調べ（S6）、そうであれば、ステップ S3 に移り、RTP パケット選択的暗号化を表わす暗号化・認証パラメータを決定して、これを通信装置 21 へ送信する（S4）。ステップ S5 で入力データが RTP パケットではないと判定され、あるいはステップ S6 で接続されている通信網 23 の伝送速度が低い移動通信網ではないと判定されると（S6）、非選択的暗号化を表わす暗号化・認証パラメータを決定して（S7）、相手通信装置 21 へ送信する（S4）。

【0018】通信装置 21 のパラメータ共有部 34 では図 3 に示すように、ステップ S7 の送信後、相手通信装置 22 から暗号化・認証パラメータを受信すると（S8）、その受信暗号化・認証パラメータが RTP パケット選択的暗号化であるかを調べ（S9）、そうであればステップ S6 に移り、暗号化・認証パラメータを、RTP パケット選択的暗号化に決定し、RTP パケット選択的暗号化でなければ暗号化・認証パラメータを非選択的暗号化に決定する（S10）。このようにしてパラメータ共有部 34 と 44 は通信路を介して暗号化範囲を共有することができる。認証範囲は入力データ（アプリケーション）にかかわらず、また通信装置 21、22 がそれぞれ接続されている通信網 23 の伝送特性に係わらず、入力データの全体とする。暗号化範囲としてはヘッダを除くか否かのみならず、暗号化範囲、認証範囲としては入力データが画像や音声である場合に、その重要部のみとすることもできる。この場合、例えばこれらデータの符号化の際に欠落すると復号が不可能となる重要なコードのみを自動的に暗号化するように指示することもできる。何れの場合も、暗号化アルゴリズムなど他のパラメータも、前記暗号化範囲の共有と同時に共有する処理を行う。

【0019】以上のようにしてパラメータが共有されると、共有された各種パラメータはパラメータ共有部 34、44 からそれぞれ暗号化・認証子付加部 33、復号化・検証部 43 へ供給される。暗号化・認証子付加部 33 において暗号化・認証子付加の処理が行われる。その手順の例を図 5 に示す。上位アプリケーション部 31 からデータパケットが入力されると（S1）、アプリケーションデータプロトコルにより、透過的に暗号化・認証子付加部 33 に入力され（S2）、このデータパケットのうち認証範囲パラメータに従って選択された部分を用いて共有した認証子生成アルゴリズム・認証子生成用鍵により認証子を生成する（S3）。認証子生成方法は、例えば、今井秀樹著「暗号のおはなし」4.7 節に詳しい。例えばハッシュ関数により認証範囲データを圧縮し、圧縮データを共通鍵で暗号化することにより生成する。その後、入力されたデータパケットに認証子を付加し（S4）、この認証子付データパケットに対し、暗号

範囲パラメータに基づいて選択部分の暗号化を共有した暗号アルゴリズム、暗号鍵を用いて施す(S5)。なおブロック暗号化を行う場合は、その固定ブロック長にデータが不足した場合に埋め合わせるパディングを暗号化の前に行う(S6)。

【0020】このようにして暗号化されたデータ構造の例を図6に示す。この例では入力されたアプリケーションデータに対し、認証子MACが付加され、アプリケーションデータ中のヘッダを除いた部分(ペイロード)と認証子とが暗号化されている。この選択的暗号化を含むデータは下位のトランスポート部32に受け渡され相手通信装置22へ伝送される。受信側通信装置22では、上記の逆の手順を用いて暗号化されたデータを復号し、データ認証子(コード)を利用して受信データの正当性を検証する。つまり図1中の通信装置22において、通信装置21から受信したパケットはトランスポート部42より復号化・検証部43に入力され、復号化・検証部43で共有した暗号化アルゴリズム、暗号化鍵、暗号化範囲に従って、この暗号化された部分が選択的に復号化され、この復号されたデータ中のデータ認証子(コード)MACを用いて、ヘッダ及び復号化されたペイロード、つまり図6中のアプリケーションデータの正当性の検証を行う。正当であれば、このアプリケーションデータをアプリケーション部41へ供給する。

【0021】このように暗号化範囲を共有することにより、入力データ中の一部を選択的に暗号化することができ、例えば安全性が問題になる部分のみを暗号化することにより、全体を暗号化する場合よりも処理量が少なく済み、しかも、安全性が問題になるおそれがない。暗号化範囲は、暗号化のための他のパラメータを共有する処理と同時に行うことができ、このための処理の増加はわずかである。特に前記例のように入力データ(アプリケーション)がRTPパケットの場合で、そのRTPパケットのヘッダ部分を暗号化しない領域とする場合は、このヘッダにUDPパケットヘッダ、IPパケットヘッダが付加されることになり、Secure RTP同様に、途中経路における、RTPパケットヘッダを含めたヘッダ圧縮に対応可能である。また、Secure RTPとは異なり、暗号化領域は通信相手との交渉によりセッション開始時に設定可能であるため、RTPパケット以外のアプリケーションにも汎用的に対応可能である。

【0022】図5では、認証子付加後に暗号化を行ったが、図7に示すように暗号化後に認証子を生成し、暗号化されたパケットに認証子を付加しても良い。この場合、受信側では、受信データの正当性を検証した後、暗号の復号化を行うことになる。以上の選択的安全化処理の流れは図8に示すようにデータが入力されると(S1)、入力データの安全化対象を示すパラメータを相手通信装置と通信路を介して共有し(S2)、その共有し

た安全化対象パラメータに従って入力データの一部に対して安全化処理を行って(S3)、相手装置へ送信する(S4)。

第2実施形態

図9にこの発明の第2実施形態を示す。これは図14に示したSSLを拡張して選択的暗号化をサポート可能としたものである。第1実施形態におけるパラメータ共有部34はさらに相手通信装置22と認証処理や暗号化・データ認証パラメータを交渉するハンドシェイク(Handshake)部34a、暗号化・データ認証パラメータを有効化するチェンジサイファ(Change Cipher)部34b、イベント・エラーを通知するアラート(Alert)部34c、そして、下位レイヤ部32を介して上記3つの各部34a、34b、34cのプロトコルデータを送受信するための第1レコード(Record)部34dからなる。第1レコード部34dのプロトコルデータフォーマットにはSSLのNレコード部と同じフォーマットを利用する。シェイクハンド部34aでは、第1レコード部34bおよび第2レコード部、つまり暗号化・認証子付加部33で利用する暗号化・データ認証パラメータを相手通信装置22と交渉して共有する。またチェンジサイファ(Change Cipher)部34bは第1レコード部34dおよび第2レコード部33の暗号化・データ認証パラメータを有効化する。つまりその暗号化を開始させて相手に通知する。第1レコード部34dには、ハンドシェイク部34aのプロトコルメッセージや選択的暗号化が不要なアプリケーションのデータが入力される。

【0023】選択的暗号化が必要なアプリケーションデータの送受信は、上記のプロトコルデータとは別に第2レコード部、つまり暗号化・認証子付加部で送受信される。第2アプリケーションデータ部38は上位の第1アプリケーション部31aのデータパケットを透過的に第2レコード部33に受け渡すためのものである。また、第1レコード部34dと異なり、第2レコード部、つまり暗号化・認証子付加部33では入力データに対して新たなヘッダは追加せず、暗号化・認証子生成処理のみを施す。第1レコード部34dで共有されたパラメータは第2レコード部33の暗号化・データ認証処理に利用される。暗号化・データ認証処理は第1実施形態と同様である。

【0024】パラメータ共有部34のハンドシェイク部34aによる相手通信装置とのパラメータ共有処理は最初は平文で通信を行うが、途中からは図15に示したデータ構造により、暗号化・認証子付加を行って、これらパラメータの共有に対しても安全化してもよい。またアプリケーションでもRTPパケットのように実時間性が要求されない、頻繁に送られない、HTTP、FTP、Telnet、RTSP(RTPのセッションを開くためのプロトコル)などのアプリケーションデータパケットは第1アプリケーション部31bより第1アプリケー

ションデータ部 37 へ通じて第 2 レコード部 34 d に入力して、これらに対しては、共有したパラメータにより暗号化をそのパケット全体に対して行い、図 15 に示したようにレコード部のヘッダ 10 を付けてレコードプロトコルパケットとしてトランスポート部 32 へ供給する。なお相手側装置 22 においては図 9 中の第 2 レコード部である暗号化・認証子付加部 33 が、復号化・検証部になり、他は同様の構成である。

第 3 実施形態

図 10 は、この発明の第 3 実施形態を示す。この実施形態では、RTSP や HTTP などの第 1 アプリケーション部 31 a を介して RTP など第 2 アプリケーション部 31 b のアプリケーションデータに対して適用される暗号化・認証子付加パラメータを共有するための通信相手との交渉をする。例えば、図 2 の暗号化パラメータを相手通信装置 22 の公開鍵で暗号化して、プロトコルメッセージボディに埋め込むことで相手通信装置 22 に伝送することができる。

【0025】1つの通信装置に暗号化・認証子付加部と復号化・検証部を合せたとしてもよい。上述においてはデータに対する安全化として暗号化と、データ認証子付加との両者を用いたが、その一方のみを用いてもよい。通信装置 21、22 の各部をコンピュータにプログラムを実行させて機能させてもよい。

【0026】

【発明の効果】以上説明したように、この発明によればデータの一部を選択的に安全化を施すことができ、かつ特定のアプリケーションに依存しない汎用的な伝送データ保護が可能であり、しかも特に移動通信に適用すればヘッダ圧縮も可能である。

*【図面の簡単な説明】

【図 1】この発明装置の実施形態の機能構成及びこの発明装置が用いられるシステム構成例を示す図。

【図 2】暗号化パラメータの例を示す図。

【図 3】送信側における暗号範囲共有処理手順の例を示す流れ図。

【図 4】受信側における暗号範囲共有処理手順の例を示す流れ図。

【図 5】図 1 中の暗号化・認証子付加部 33 の処理手順の例を示す流れ図。

【図 6】図 1 中の暗号化・認証子付加部 33 の出力パケットのデータ構造の例を示す図。

【図 7】暗号化・認証子付加部 33 の処理手順の他の例を示す流れ図。

【図 8】この発明の方法の処理手順の例を示す流れ図。

【図 9】この発明装置の第 2 実施形態の機能構成を示す図。

【図 10】この発明装置の第 3 実施形態の機能構成を示す図。

【図 11】選択的暗号化されたパケットのデータ構造を示す図。

【図 12】A は Secure RTP を使用しない処理を示す図、B は Secure RTP を使用する時の処理を示す図である。

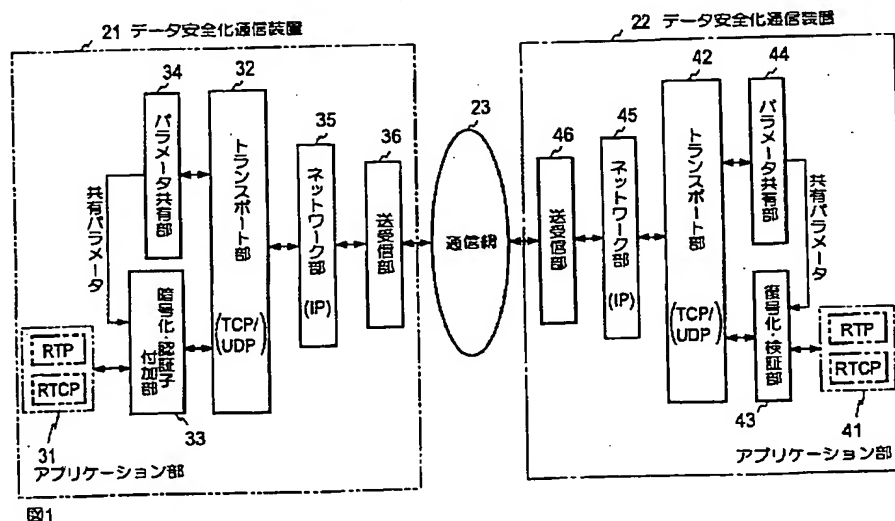
【図 13】A は SSL/WTLS を使用しないアプリケーションデータの処理を示す図、B は SSL/WTLS を使用する時の処理を示す図である。

【図 14】SSL/WTLS レイヤの詳細を示す図。

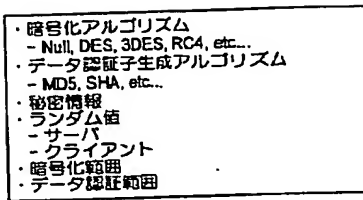
【図 15】SSL/WTLS により処理されたレコード

* 30 プロトコルデータの構造を示す図。

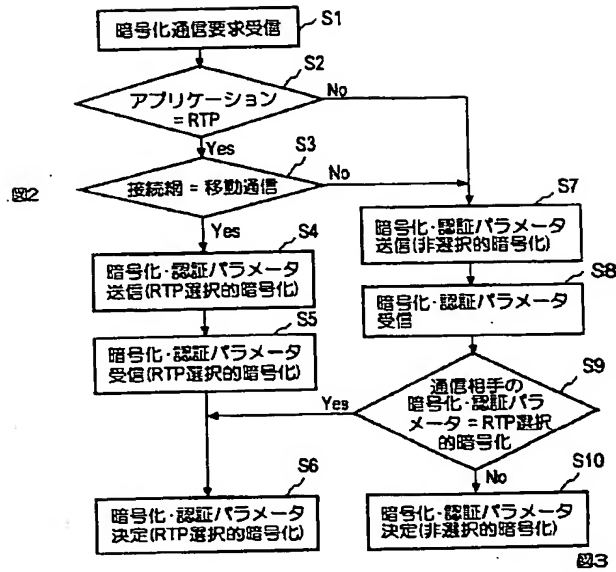
【図 1】



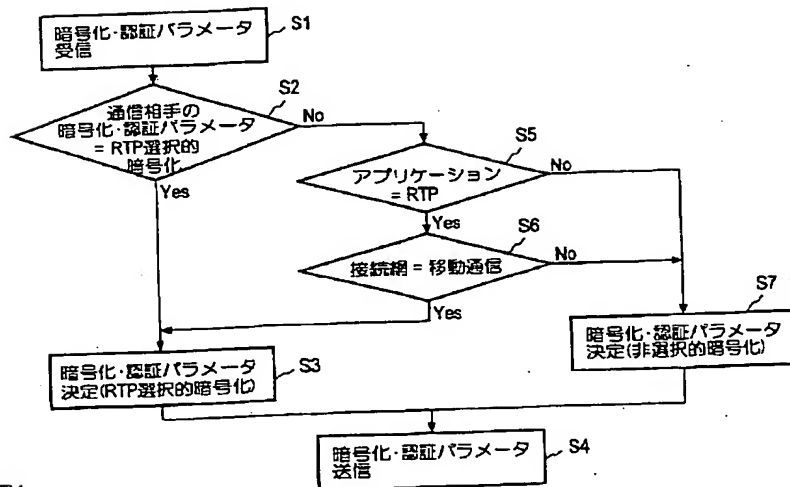
【図 2】



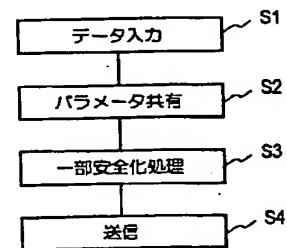
【図 3】



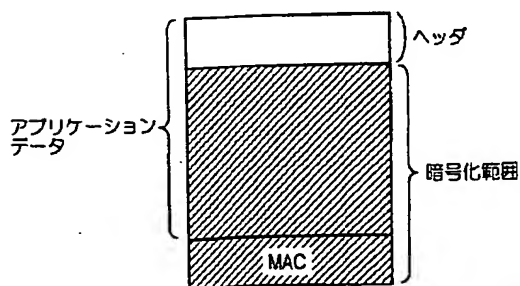
【図 4】



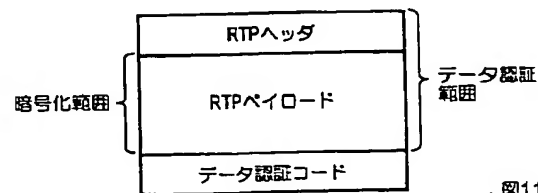
【図 8】



【図 6】



【図 11】



【図 5】

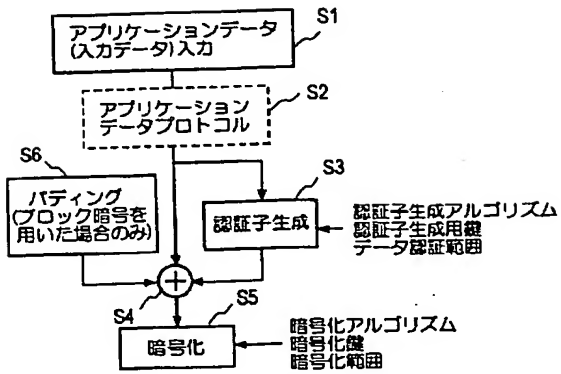


図5

【図 7】

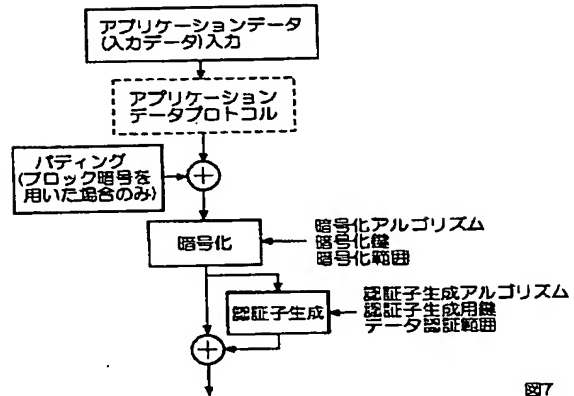


図7

【図 9】

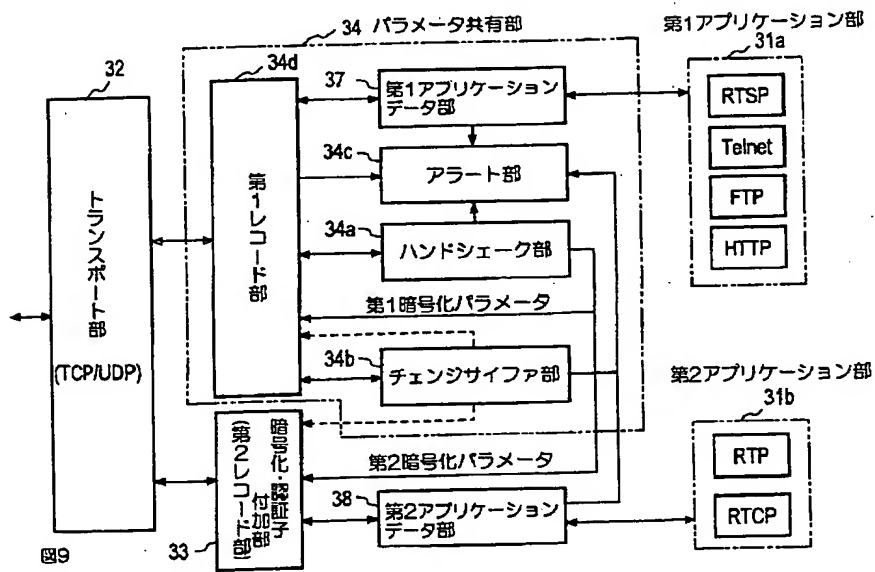


図9

【図 12】

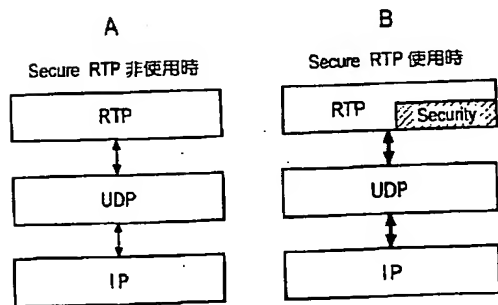


図12

【図 13】

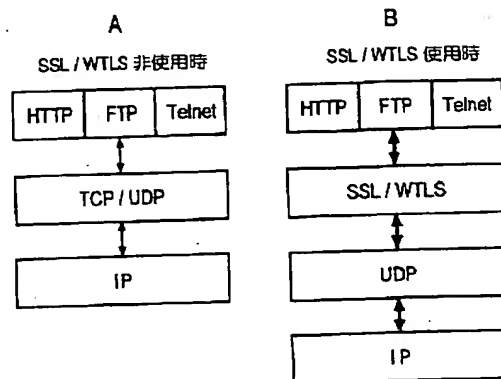
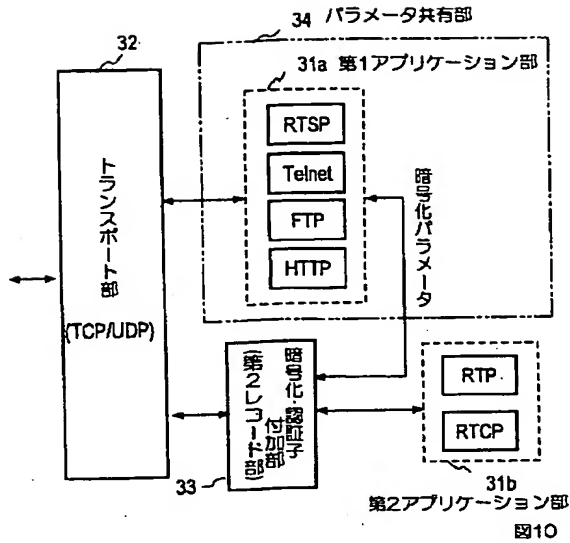


図13

【図10】



【図14】

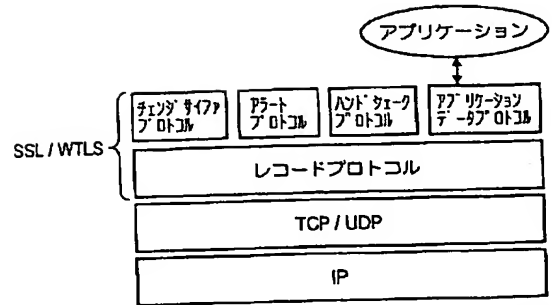


図14

【図15】

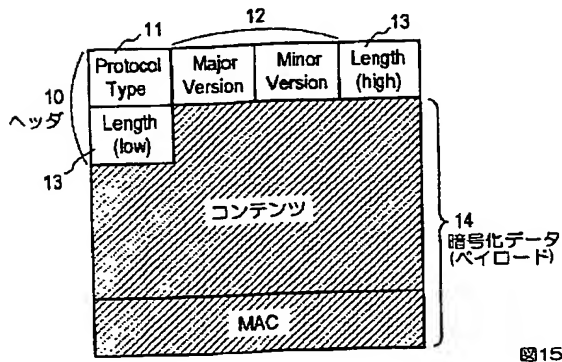


図15

BEST AVAILABLE COPY